CLIENT ALERT

Supreme Court Resolves Circuit Split over Scope of Computer Fraud and Abuse Act

Jun.04.2021

After months of anticipation, the Supreme Court issued its opinion in *Van Buren v. United States* narrowing the scope of what constitutes "exceeds authorized access" under Section 1030(a)(2) of the Computer Fraud and Abuse Act ("CFAA"). No. 19-783, --- S.Ct. --- (June 3, 2021). The Supreme Court ruled that to be liable under the "exceeds authorized access" prong of the CFAA, a defendant must have accessed information within a computer system they were not permitted to access. It is no longer sufficient under the CFAA to show a defendant had an improper motive to obtain and use information on a computer system which they were permitted to access.

The CFAA makes it illegal to access a computer without authorization or "to access a computer ***with*** authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *See generally* Section 1030(a). At issue in *Van Buren* is whether a person who is authorized to access information on a computer for certain purposes exceeds that access under Section 1030(a)(2) if he accesses the same information for an improper purpose. *Van Buren* involved a police officer who accessed a law-enforcement database to obtain information for private, rather than legitimate law-enforcement, use.

The CFAA is a criminal statute that includes a private right of action, and thus the case law has developed in both the criminal and civil contexts. The CFAA defines "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This definition has led to a circuit split on what type of conduct actually constitutes a CFAA violation. In particular, and as we have discussed here, courts have grappled with whether the CFAA focuses on how the individual ***accesses*** the information, as opposed to how or under what circumstances the individual ***uses*** it.

The First, Fifth, Seventh, and Eleventh Circuits broadly interpret "exceeds authorized access" to include using information on a computer in violation of a confidentiality agreement, or accessing information on a computer for a purpose prohibited by an employer. Specifically, the Eleventh Circuit has held that a defendant "exceeded his authorized access" under the CFAA by improperly using information that he was authorized to access. *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). In contrast, the Second, Fourth, and Ninth Circuits have adopted a narrower interpretation of "exceeding authorized access": liability cannot be imposed on a person with permission to access information on a computer who then uses that information for an improper purpose. *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (holding that subsequent improper use of information that was acquired by individuals with authorization to access such information is not a CFAA violation).

In a 6-3 ruling, the Court sided with the Second, Fourth, and Ninth Circuits in holding that an individual "exceeds authorized access" when she accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to her. In so holding, the Court narrowed the scope of the CFAA and resolved the circuit split. The Court adopted the narrow approach, focusing on one's authority to *access* information

(i.e., the act) on a device rather than one's authority to *use* that information. Justice Barrett, writing for the majority, found that the CFAA does not cover those who "have improper motives for obtaining information that is otherwise available to them."

Justice Barrett, joined by the other two Trump appointees and the Court's liberal wing, applied a textualist approach in interpreting the CFAA. Of critical importance was the meaning of "so" contained in the clause "entitled so to obtain." In analyzing the plain meaning of the word, Justice Barrett held the phrase is "best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access." Any other interpretation, the Court held, "would attach criminal penalties to a breathtaking amount of commonplace computer activity."

Justice Barrett's opinion focuses on an individual's authority to access systems that host information, rather than the individual's authority to possess or use that information. As the Court's first foray into the CFAA, this decision will have far-reaching implications for any individual or business operating in the digital domain, as the scope of civil and criminal liability under the CFAA can impact just about any sort of relationship involving access to computer systems, whether it be employer-employee relationships or third-party relationships, such as visitors to a website.

Businesses seeking to curb unauthorized use of information by employees and others may need to revisit how and under what circumstances they grant access to such information. It is clear, however, that businesses will have a narrower set of legal tools to prevent unauthorized use of certain information. Instead, businesses must resort to other legal tools to prevent such conduct. For example, the federal Defend Trade Secrets Act (DTSA) and state trade secret, tort, trespass, contract law, and, depending on the circumstances, intellectual property law will take on more significance in holding individuals liable for access to and use of the information. In addition, businesses could bolster their contract claims by imposing greater restrictions on access or use of information in contracts, terms of service, or business handbooks. The government likewise will be more constrained in the types of cases is prosecutes using the CFAA.

In addition to *Van Buren*, a second CFAA case, *HiQ v. LinkedIn*, is pending before the Supreme Court. That case involves a business using automated bots to scrape information from public LinkedIn profiles including name, work history, job titles and skills, and using that information to yield "people analytics" in order to sell such information to its clients. While the Supreme Court has not ruled on LinkedIn's pending cert petition, the Court's approach to the CFAA in *Van Buren* will undoubtedly impact companies relying on, or opposing, data scraping (or other technical measures to obtain information) as a business model. The ultimate outcome in the *HiQ* case will undoubtedly be influenced by the Court's approach to the CFAA in *Van Buren*.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Nimrod Haim Aviad
Partner – Los Angeles
Phone: +1 213.443.5534
Email: naviad@crowell.com

Stephen M. Byers
Partner – Washington, D.C.
Phone: +1 202.624.2878
Email: sbyers@crowell.com

Mark A. Klapow

Partner – Washington, D.C.
Phone: +1 202.624.2975
Email: mklapow@crowell.com

Anne Elise Herold Li
Partner – New York
Phone: +1 212.895.4279
Email: ali@crowell.com

Kayvan M. Ghaffari
Counsel – San Francisco
Phone: +1 415.365.7223
Email: kghaffari@crowell.com

Raija Horstman
Counsel – Los Angeles
Phone: +1 213.443.5530
Email: rhorstman@crowell.com

Julia Milewski
Counsel – Washington, D.C.
Phone: +1 202.624.2514
Email: jmilewski@crowell.com

Joshua M. Rychlinski
Counsel – Washington, D.C.
Phone: +1 202.624.2688
Email: jrychlinski@crowell.com